НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання лабораторної роботи

ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ СИСТЕМ WEBMONEY, PAYPAL

Виконали студентки
групи ФІ-32мн
Зацаренко А.Ю.
Футурська О.В.

Київ — 2024

ЗВІТ

1.1 Мета лабораторної роботи

Дослідження особливостей реалізації криптографічних механізмів платіжних систем.

1.2 Постановка задачі

Дослідити особливості реалізації криптографічних протоколів, а також особливості роботи з електронними гаманцями систем WebMoney та PayPal. Звіт має містити детальний опис проведеного дослідження особливостей реалізації криптографічних механізмів протоколів систем WebMoney та PayPal. Також звіт має містити загальні теоретичні відомості побудови платіжних систем та їх основні характеристики (специфікація SET), зокрема систем мікроплатежів, таких як Payword та Micromint, та протоколи електронних грошей. Для кожної наведеної системи або протоколу необхідно обґрунтувати його захищеність та вибір криптографічних примітивів.

1.3 Хід роботи

Платіжна система — це сукупність інструментів, процедур і правил, які забезпечують переказ грошей між учасниками. Вона включає платіжні інструменти (карти, чеки, електронні гроші), інфраструктуру (банки, платіжні шлюзи, мережі обміну даними) і механізми безпеки.

1.3.1 Основні компоненти платіжної системи

1) **Користувачі (учасники):** Фізичні та юридичні особи, які здійснюють платежі (покупці, продавці);

2) **Фінансові установи:** Банки-емітенти (які випускають платіжні картки) та банки-еквайри (обслуговують платежі продавців);

3) **Платіжні інструменти:** Засоби для проведення розрахунків, наприклад:

– Платіжні картки (дебетові, кредитні);

– Електронні гроші;

– Мобільні додатки;

4) **Інфраструктура:** Мережі передачі даних, сервери авторизації, термінали;

5) **Правила та стандарти:** Регулюють функціонування системи. Наприклад **Payment Card Industry Data Security Standard** (PCI DSS) — стандарт безпеки даних індустрії платіжних карток, розроблений Радою зі стандартів безпеки індустрії платіжних карток (Payment Card Industry Security Standards Council, PCI SSC), заснованою міжнародними платіжними системами Visa, MasterCard, American Express, JCB і Discover. Стандарт являє собою сукупність 12 деталізованих вимог щодо забезпечення безпеки даних про власників платіжних карток, які передаються, зберігаються і обробляються в інформаційних інфраструктурах організацій;

6) **Механізми безпеки:** Протоколи шифрування, двофакторна автентифікація, тощо.

1.3.2 Основні характеристики платіжних систем

Платіжні системи є важливими інструментами для проведення фінансових операцій, забезпечуючи зручність, швидкість і безпеку.

✏ **Доступність** — платіжні системи повинні бути доступними для користувачів у будь-який час доби. Це означає, що вони повинні працювати 24/7 без перерв, що дозволяє здійснювати платежі та перекази в будь-який момент. Наприклад, такі системи, як EasyPay, забезпечують безперервний доступ до своїх послуг, що робить їх зручними для користувачів;

✏ **Швидкість транзакцій** — швидкість обробки платежів є критично важливою характеристикою платіжних систем. Багато з них

пропонують миттєві транзакції, що дозволяє користувачам отримувати підтвердження платежу за лічені секунди. Наприклад, сучасні платіжні системи можуть обробляти міжнародні перекази за короткий час завдяки оптимізації процесів;

✏ **Надійність** — здатність забезпечувати стабільну роботу без збоїв і втрат даних. Важливо, щоб система могла обробляти великі обсяги транзакцій без затримок і помилок. Це також включає в себе резервування даних та використання надійної інфраструктури для запобігання збоям;

✏ **Безпека** — захист даних користувачів від шахрайства та витоків інформації. Для цього використовуються сучасні технології шифрування та аутентифікації, такі як SSL-протоколи (англ. Secure Sockets Layer) і біометрична автентифікація. Наприклад, платіжні системи проходять регулярні перевірки на відповідність міжнародним стандартам безпеки;

✏ **Інтероперабельність** — можливість платіжних систем взаємодіяти з іншими фінансовими інститутами та платформами. Інтероперабельність дозволяє користувачам здійснювати транзакції між різними системами без додаткових ускладнень. Це особливо важливо в умовах глобалізації фінансових послуг;

✏ **Масштабованість** — здатність адаптуватися до зростаючих обсягів транзакцій без втрати продуктивності. Це важливо для бізнесу, який може швидко розширювати свої операції і потребує надійної платіжної інфраструктури для підтримки зростаючих потреб клієнтів.

1.3.3 Специфікація SET (Secure Electronic Transaction)

SET — це протокол, розроблений у 1996 році компаніями Visa, Mastercard, IBM, Microsoft та іншими для забезпечення безпеки онлайн-платежів. Він забезпечує шифрування транзакцій і автентифікацію учасників.

Основні характеристики SET:

1) **Безпека транзакцій:**

✓ Використання асиметричного шифрування (RSA) для передачі даних.

✓ Симетричне шифрування (DES) для забезпечення конфіденційності транзакцій.

✓ Протокол SSL/TLS для передачі даних у зашифрованому вигляді.

2) **Аутентифікація учасників:**

✓ Кожен учасник (покупець, продавець, банк) має цифровий сертифікат, виданий сертифікаційним центром (CA).

✓ Підтвердження особи через сертифікати.

3) **Конфіденційність даних:**

✓ Дані платіжної картки покупця недоступні продавцю, передаються безпосередньо банку.

✓ Розділення інформації: продавець бачить лише дані замовлення, банк — лише платіжні дані.

4) **Цілісність даних:** гарантії, що дані залишаються незмінними під час передачі між учасниками транзакції, використовуючи механізми шифрування, електронні підписи та контрольні суми, які дозволяють виявити будь-які спроби зміни чи спотворення інформації. .

5) **Протидія шахрайству:** ряд заходів і технологій, спрямованих на виявлення та запобігання несанкціонованому доступу до чутливих даних. Це включає:

✓ Електронні підписи: Використовуються для підтвердження особи учасників транзакції;

✓ Захищене управління ключами: Застосування інфраструктури відкритих ключів (PKI) для управління та розподілу ключів;

✓ Багатофакторна аутентифікація: Використання декількох методів аутентифікації (наприклад, паролі + SMS-коди) для підтвердження особи користувача перед виконанням транзакцій.

Основні етапи роботи SET:

1) **Реєстрація учасників:** Всі учасники отримують сертифікати від сертифікаційного центру CA.

2) **Ініціація транзакції:**

❄ Покупець надсилає замовлення продавцю, а також зашифровані платіжні дані.

❄ Продавець передає платіжні дані банку через мережу.

3) **Авторизація платежу:**

❄ Банк перевіряє автентичність сертифікатів та наявність коштів.

❄ Підтвердження або відхилення платежу.

4) **Завершення транзакції:**

❄ Підтвердження продавцю про успішний платіж.

❄ Передача товару/послуги покупцю.

Переваги SET:

→ Високий рівень безпеки завдяки цифровим сертифікатам і шифруванню;

→ Захист даних покупця від продавця;

→ Унеможливлення перехоплення чи підробки транзакцій.

Недоліки SET:

→ Складність впровадження через необхідність сертифікації всіх учасників;

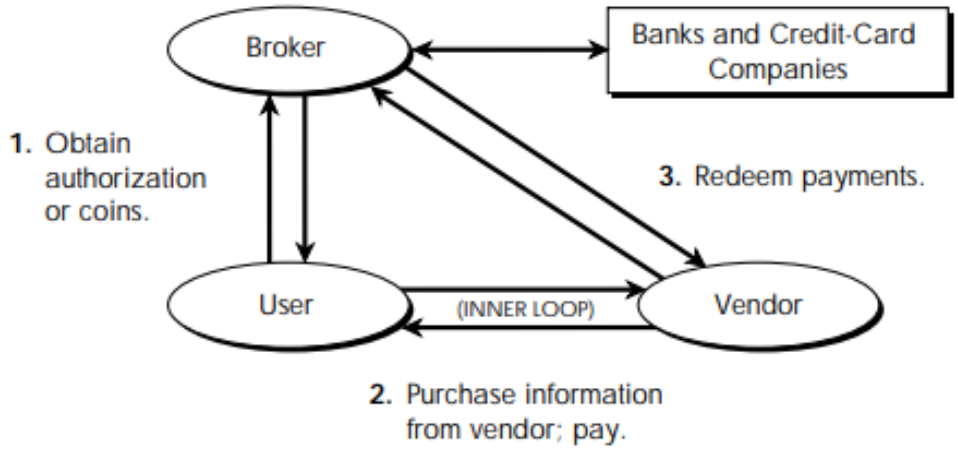
→ Високі витрати на підтримку;

→ Низька популярність через розвиток інших спрощених і ефективних протоколів.

1.3.4 Характеристики Payword та Micromint

Схеми мікроплатежів — це особливий вид платіжних схем для додатків, в яких кожен платіж дуже малий. Для підтримки мікроплатежів потрібна виняткова ефективність, інакше вартість механізму перевищить

вартість платежів. PayWord і MicroMint — дві прості схеми мікроплатежів. В обох схемах учасниками є брокери, користувачі та продавці. Брокери уповноважують користувачів здійснювати мікроплатежі продавцям і викуповують платежі, зібрані продавцями. Відносини між брокером і користувачем та брокером і продавцем є довгостроковими, тоді як відносини між користувачем і продавцем є тимчасовими.



Payword — це система мікроплатежів, яка спрощує проведення численних дрібних транзакцій, використовуючи концепцію криптографічних ланцюжків. Її ключові особливості:

1) **Попередня авторизація та довіра:** Перед початком транзакцій користувач (покупець) отримує сертифікат від довіреної третьої сторони (наприклад, банку чи платіжного оператора), який підтверджує його платоспроможність. Цей сертифікат служить основою довіри між покупцем і продавцем.

2) **Криптографічний ланцюжок:** Користувач генерує послідовність унікальних цифрових значень («paywords») за допомогою геш-функції. Кожне значення в ланцюжку залежить від попереднього, що забезпечує їх унікальність і автентичність.

3) **Механізм платежів:** При кожній покупці користувач передає продавцю наступний «payword» із ланцюжка. Це спрощує процес, оскільки немає потреби звертатися до банку або платіжної системи для

підтвердження кожної транзакції.

4) **Акумуляція платежів:** Продавець накопичує отримані «paywords» і після завершення періоду або при досягненні певної суми звертається до банку для їхнього обміну на реальні кошти.

5) **Економія ресурсів:** Використання геш-функцій дозволяє зменшити обчислювальні витрати, оскільки кожна транзакція вимагає мінімальних обчислень з боку продавця та не потребує додаткової авторизації в реальному часі.

6) **Безпека:** Завдяки криптографічній природі геш-функцій, підробити або змінити ланцюжок «paywords» неможливо.

Micromint — це мікроплатіжна система, яка базується на використанні криптографічно згенерованих «монет» для спрощення платежів. Вона має такі основні риси:

1) **Генерація монет:** Монети створюються шляхом виконання складних криптографічних обчислень, наприклад, через пошук геш-значень із заданими властивостями (подібно до процесу майнінгу в криптовалютах). Генерація відбувається централізовано, що гарантує контроль за випуском монет і їхню унікальність.

2) **Економічна модель:** Витрати на створення «монет» значні лише на етапі генерації, після чого їхнє використання стає дуже дешевим. Продавці не потребують додаткових перевірок кожної транзакції, оскільки монети вважаються автентичними за замовчуванням.

3) **Анонімність:** Монети не пов'язані з особистими даними користувачів, що забезпечує конфіденційність транзакцій.

4) **Простота використання:** Покупець отримує набір монет і використовує їх для оплати товарів чи послуг. Продавець приймає монети без необхідності перевіряти покупця чи підтверджувати операцію в реальному часі.

5) **Незалежність транзакцій:** Кожна «монета» є автономною і може використовуватися незалежно від інших. Це дозволяє легко проводити

транзакції між різними сторонами без постійного зв'язку з «центру».

6) **Захист від шахрайства:** Завдяки криптографії підробка монет є надзвичайно складною і нерентабельною.

Порівняння Payword та Micromint:

✏ **Тип транзакцій:** Payword ефективний для послідовних платежів одному продавцю, тоді як Micromint більше підходить для одноразових транзакцій із різними продавцями.

✏ **Анонімність:** Micromint забезпечує повну анонімність, тоді як Payword передбачає використання сертифікатів, що ідентифікують користувача.

✏ **Витрати:** У Payword витрати зменшуються за рахунок зниження кількості взаємодій із банком, а в Micromint — завдяки одноразовій генерації монет.

✏ **Сфера застосування:** Payword підходить для послуг із багаторазовими платежами (передплата, ігри), а Micromint — для покупки цифрового контенту чи дрібних товарів.

1.3.5 Протоколи електронних грошей

Протоколи електронних грошей варіюються від централізованих рішень (наприклад, PayPal) до децентралізованих систем (Bitcoin, Etherium) і спеціалізованих протоколів для мікроплатежів (Payword, Micromint). Кожен із них має свої переваги й недоліки залежно від вимог до анонімності, масштабованості, безпеки та ефективності.

Chaum's e-Cash, розроблений Девідом Чаумом у 1983 році, є одним із перших протоколів електронних грошей, що забезпечує анонімність і безпечні транзакції в цифровому середовищі. Цей протокол став основою для подальшого розвитку електронних платіжних систем і криптовалют.

❄ **Анонімність:** Використовує сліпі підписи (англ. blind signatures), що дозволяють банкам підтверджувати «монети», не знаючи, власне, самого користувача.

❄ **Процес роботи:**

– Користувач отримує у банку зашифровану «монету».

– Монета підписується банком і стає придатною для використання.

– При оплаті користувач розшифровує монету та передає її продавцю, який перевіряє її автентичність у банку.

❄ **Недолік:** Складність впровадження через високі вимоги до обчислювальних потужностей.

Протокол Bitcoin і Etherium, розроблені як децентралізовані системи електронних грошей, які використовують блокчейн.

– **Децентралізація:** Всі транзакції зберігаються у відкритому реєстрі (блокчейні), доступному для всіх учасників мережі.

– **Прозорість:** Кожен може перевірити транзакції, але справжня ідентичність користувачів прихована за псевдонімами (адресами).

– **Безпека:** Ґрунтується на криптографічному доказі роботи (Proof-of-Work для Bitcoin і Proof-of-Stake для Etherium).

– **Недоліки:** Повільність обробки транзакцій і велика енергозатратність (Bitcoin).

1.3.6 Криптографічні механізми у WebMoney та PayPal

Система WebMoney

WebMoney — це система електронних грошей, яка дозволяє користувачам здійснювати фінансові операції онлайн, зокрема проводити мікроплатежі, обмін валют, а також зберігати електронні кошти. Це система електронних розрахунків, заснована в 1998 році і належить WM Transfer Ltd. Технічна підтримка та розробка програмного забезпечення знаходиться в Росії. Однак, WebMoney не зареєстрована в Росії як система електронних платежів, оскільки, з юридичної точки зору, титульні знаки не є електронними грошима.

У платіжних системах, таких як WebMoney, титульні знаки можуть

позначати певні одиниці вимірювання або спеціальні сертифікати. Наприклад, в WebMoney користувачі можуть працювати з титульними знаками у вигляді віртуальних валют (WMZ, WMR, WMU тощо), які фактично є одиницями електронних грошей, еквівалентними національним валютам. Ці знаки виступають як відображення віртуальних коштів у системі. WebMoney є більш популярним в СНД, однак її користувачі з усього світу можуть використовувати систему для проведення фінансових операцій. В Україні із 24 травня 2018 року сервіс WebMoney знаходиться під забороною.

WebMoney використовує унікальну модель взаємодії користувачів і серверів для забезпечення безпеки транзакцій. Основними елементами криптографічного захисту є:

1) **Аутентифікація через ключі:**

– Кожен користувач має індивідуальний криптографічний ключ (WMID — 12-тизначна цифрова послідовність), який зберігається на пристрої користувача або в апаратних токенах. WebMoney дозволяє користувачам зберігати анонімність, оскільки система працює за принципом ідентифікації через WMID (унікальний ідентифікатор), а не через реальні дані користувача.

– Для підписання операцій використовується алгоритм електронного підпису (ECDSA або RSA). Використання цифрового підпису гарантує автентичність операцій, оскільки тільки власник ключа може їх виконати.

2) **Шифрування даних:**

– Передача даних між клієнтом і сервером здійснюється через захищені протоколи (HTTPS з використанням TLS). Шифрування через TLS запобігає перехопленню даних під час передачі.

– Для захисту внутрішньої комунікації використовується симетричне шифрування (AES).

3) **Двофакторна автентифікація:** Можливість підключення додаткових методів аутентифікації, таких як одноразові паролі (OTP) або SMS-коди. Сегментація транзакцій і багатоетапна перевірка знижують

ризики шахрайства.

4) **Система підтверджень:** Транзакції повинні бути підписані цифровим підписом користувача та підтверджені сервером WebMoney, який перевіряє валідність ключів.

Недоліки:

❄ **Анонімність:** Через відсутність обов'язкової ідентифікації є ризик шахрайства.

❄ **Обмеження у міжнародних транзакціях:** Хоча WebMoney використовується в різних країнах, вона не так широко підтримується, як інші системи (наприклад, PayPal).

Система PayPal

PayPal є однією з найбільших платіжних систем у світі, що дозволяє здійснювати електронні платежі та перекази між користувачами, а також для онлайн-покупок. Система активно використовується в Європі, Північній Америці та багатьох інших країнах для оплат за товари, послуги та обміну валют.

Для користування PayPal необхідно створити обліковий запис, який пов'язується з реальними банківськими картками або банківським рахунком. Це знижує анонімність порівняно з WebMoney. PayPal використовує високий рівень шифрування даних, а також захищає покупців за допомогою політики захисту покупця (Buyer Protection), що повертає гроші за неправомірно надані послуги або товар.

PayPal побудований на централізованій архітектурі з акцентом на конфіденційності та простоті для користувача. Централізована архітектура забезпечує строгий контроль за всіма транзакціями. Основними елементами криптографії є:

1) **Шифрування даних:**

– Використання HTTPS (TLS 1.2/1.3) для захищеного з'єднання між клієнтом і сервером.

– Шифрування даних на сервері за допомогою AES-256.

2) **Автентифікація користувача:**

– Логін і пароль із можливістю підключення двофакторної автентифікації (2FA).

– В деяких випадках використовується біометрична автентифікація (відбитки пальців або розпізнавання обличчя).

3) **Контроль транзакцій:**

– Кожна транзакція перевіряється на рівні серверів за допомогою криптографічного підпису.

– Використовується HMAC (SHA-256) для перевірки цілісності даних і підтвердження автентичності запитів API.

Недоліки:

❄ **Комісії:** PayPal стягує комісії з продавців за використання платіжної системи, а також за міжнародні перекази.

❄ **Залежність від інтернет-з'єднання:** Як і в будь-якій онлайн-системі, без доступу до інтернету система не працюватиме.

ВИСНОВКИ

SET був одним із перших протоколів, що надавали повний захист транзакцій в інтернеті. Проте з часом його витіснили простіші у впровадженні методи, які забезпечують схожий рівень безпеки, але з меншими витратами.

Payword найбільше підходить для ситуацій, коли один користувач здійснює багато дрібних транзакцій із тим самим продавцем, наприклад, у системах передплати або цифрових послуг.

Micromint підходить для систем із великою кількістю дрібних, одноразових платежів, наприклад, для оплати статей, музики або доступу до контенту на платформах.

WebMoney підходить для анонімних транзакцій і має високий рівень захищеності завдяки використанню цифрових підписів і криптографічних ключів. PayPal орієнтований на зручність і масштабованість, використовуючи перевірені криптографічні механізми для захисту даних у централізованій системі.

Обидві системи забезпечують захищеність завдяки використанню сучасних криптографічних примітивів, таких як AES, RSA і HMAC, однак WebMoney краще підходить для користувачів, які потребують вищого рівня анонімності.